

**Notice of Allowability**

Application No.

09/717,524

Examiner

Ronald Baum

Applicant(s)

SKIBBIE ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 9/2/2005.
2. ☒ The allowed claim(s) is/are 1,3,5-22,25.
3. ☐ The drawings filed on \_\_\_\_\_ are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 2/2/2005.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joseph R. Burwell, Reg. No. 44,468 on 2/2/2005.

1. Replace claims 1,3,11,17 and 22 with:

1. A method for executing a signed applet packaged in a given file, comprising:
  - upon loading a class, determining whether a signature in the given file type applies to the class;
  - if so, executing a verification procedure to verify the signature and the identity of a signer that generated the signature;
  - following a successful verification, determining whether the signer is identified in a policy entry;
  - if the signer is identified in the policy entry, populating a permission set for the class;
  - wherein the signature is verified using a given algorithm used to sign the applet; and

wherein the step of populating the permission set for the class awards the class a permission as specified in the policy entry.

3. The method as described in Claim 1 wherein the given algorithm is selected from the set of algorithms consisting of

DSA/SHA1,

RSA/MD5 and

RSA/SHA1.

11. A method for executing a signed applet packaged in a given file, comprising:

upon loading each class, determining whether any signatures in the given file applies to the class;

if so, executing a verification procedure to verify the signature and the identity of a signer that generated the signature;

following a successful verification, determining whether the signer is identified in a policy entry;

if the signer is identified in the policy entry, awarding the class a permission as identified in the policy entry;

responsive to a request that requires a permission, using the permission set for the class to determine whether the class has the permission; and

wherein the signature is verified using a given algorithm used to sign the applet.

Art Unit: 2136

17. A computer program product on a computer readable media including computer usable code for use in a Java runtime environment (JRE), comprising:

- an applet class loader for loading a set of applet classes archived in a signed file;

- a set of signature engine classes for verifying applet class signatures;

- a security manager class callable by the applet class loader upon receipt of an initial request that requires a given permission and, in response thereto invoking a policy file class that verifies a signer based on the existence of a matching certificate in a set of keystores;

- wherein at least one signature engine verifies signatures using a given algorithm used to sign the applet classes archived in a signed file; and

- wherein for populating a permission set for the class, wherein the class is awarded a permission as specified in the policy file class managed by the security manager class.

22. A system, comprising:

- a browser;

- a Java runtime environment;

- a set of keystores;

- an applet class loader for loading a set of applet classes archived in a signed file;

- a set of signature engine classes for verifying applet class signatures;

a security manager class callable by the applet class loader upon receipt of an initial request that requires a given permission and, in response thereto, invoking a policy file class that verifies a signer based on the existence of a matching certificate in the set of keystores;

a means for populating a permission set for the class, wherein the class is awarded a permission as specified in a policy entry in a database managed by the security manager class; and

wherein at least one signature engine verifies signatures using a given algorithm used to sign the applet.

2. Cancel claims 2,4,23,24.

***Examiner's Statement of Reasons for Allowance***

3. Claims 1,3,5-22,25 are allowed over prior art.
4. This action is in reply to applicant's correspondence of 02 September 2004.
5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
6. As per claims 1,11,17, and 22, prior art of record, Devine et al, U.S. Patent 6,598,167 B2, fails to teach, alone, or in combination, of;

(Claim 1) "A method for executing a signed applet packaged in a given file, comprising:

upon loading a class, *determining whether a signature in the given file type applies to the class*;

if so, executing a verification procedure to *verify the signature and the identity of a signer* that generated the signature;

following a successful verification, *determining whether the signer is identified in a policy entry*;

if the signer is identified in the policy entry, *populating a permission set for the class*;

wherein the signature is verified using a *given algorithm used to sign the applet*; and

wherein the step of populating the permission set for the class *awards the class a permission as specified in the policy entry*.”

(Claim 11) “A method for executing a signed applet packaged in a given file, comprising:

upon loading each class, *determining whether any signatures in the given file applies to the class*;

if so, executing a verification procedure to *verify the signature and the identity of a signer* that generated the signature;

following a successful verification, *determining whether the signer is identified in a policy entry*;

if the signer is identified in the policy entry, *awarding the class a permission as identified in the policy entry*;

responsive to a request that requires a permission, *using the permission for the class to determine whether the class has the permission*; and

wherein the signature is verified using a *given algorithm used to sign the applet*.”

(Claim 17) “A computer program product including computer usable code for use in a Java runtime environment (JRE), comprising:

an applet class loader for loading a set of applet classes archived in a signed file;

a set of signature engine classes for verifying applet class signatures;

a *security manager class callable by the applet class loader* upon receipt of an initial request that requires a given permission and, in response thereto *invoking a policy file class that verifies a signer based on the existence of a matching certificate in a set of keystores*;

wherein at least one signature engine verifies signatures using a *given algorithm used to sign the applet classes archived in a signed file*; and

wherein for populating a permission set for the class, wherein the class is *awarded a permission as specified in the policy file class* managed by the security manager class.”

(Claim 22) “A system, comprising:

- a browser;
- a Java runtime environment;
- a set of keystores;
- an applet class loader for loading a set of applet classes archived in a signed file;
- a set of signature engine classes for verifying applet class signatures;
- a security manager class callable by the applet class loader upon receipt of an initial request that requires a given permission and, in response thereto, invoking a policy file class that verifies a signer based on the existence of a matching certificate in the set of keystores;*
- a means for populating a permission set for the class, wherein the class is *awarded a permission as specified in a policy entry in a database managed by the security manager class;* and
- wherein at least one signature engine verifies signatures using *a given algorithm used to sign the applet.*”

7. The *italicized* above claim elements dealing with (for example; claim 1) “ ... *determining whether a signature in the given file type applies to the class ... verify the signature and the identity of a signer ... determining whether the signer is identified in a policy entry ... populating a permission set for the class ... given algorithm used to sign the applet ... awards the class a permission as specified in the policy entry.* ” serving to patently distinguish the



Art Unit: 2136

invention from prior art. Specifically, while the use of alternate applet class packaging per se on a developer/user browser requirements basis (i.e., ".CAB", ".JAR" file, signature verification database/certificate and associated development/module assembly software tools/technologies) is known in the prior art (i.e., see Griscom, Daniel, "Code Signing for Java Applets", Daniel T. Griscom Web site "[http://www.boran.com/security/Doc\\_CodeSigning.html#both](http://www.boran.com/security/Doc_CodeSigning.html#both)", 1998, entire document), the use of an single integrated framework that via signature verification (of the signer) builds a permission structure (i.e., a set) usable during applet run time/user utilization (at which permission is a function of the original policy associated now with the verified signer identity), is patently distinct in the art. Further, the use of the Java Plug-in module part of the supplied (with the Java Runtime Environment) to effect a partial multi-browser environment is also known in the art; finding specific utilization in limited instances where the JDK/Netscape environments dominate the applications/WEB services (i.e., see disclosure, pp. 1-3), but the single integrated environment of the applicants invention clearly negates the need for such limited solutions.

As per the applicants arguments in the previous remarks in the Amendment (September 02, 2004), the examiner finds the applicant's arguments to be persuasive in that the art of record (Devine et al) does not teach or suggest the use of an integrated framework for executing a signed applet packaged in a given file utilizing the said claimed aspects and limitations as recited above. These aspects serving to patently distinguish the invention from the prior art of record.

Prior art of record specifically deals with said partial limited solutions. There is nowhere implicitly or explicitly any mention of integrated, let alone a framework (i.e., the developing/packaging and user runtime/browser/verification/permission) oriented environment.

Art Unit: 2136

However, the claim language clearly associates the applicant's invention to the Java based technologies per se. This is in contrast to object oriented software/environments and technologies in general (i.e., ".NET", C++, etc.).

Claim 11 deals with permission per se (versus the permission set aspect of claim 1) and subsequent user use/running thereof, of the applet and associated class aspects.

8. Claims 17,22 deal with the software embodiment and system aspects of the methods of claim 1.

9. Dependent claims 3,5-10,12-16,18-21, and 25 are allowable by virtue of their dependencies.


### ***Conclusion***

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100